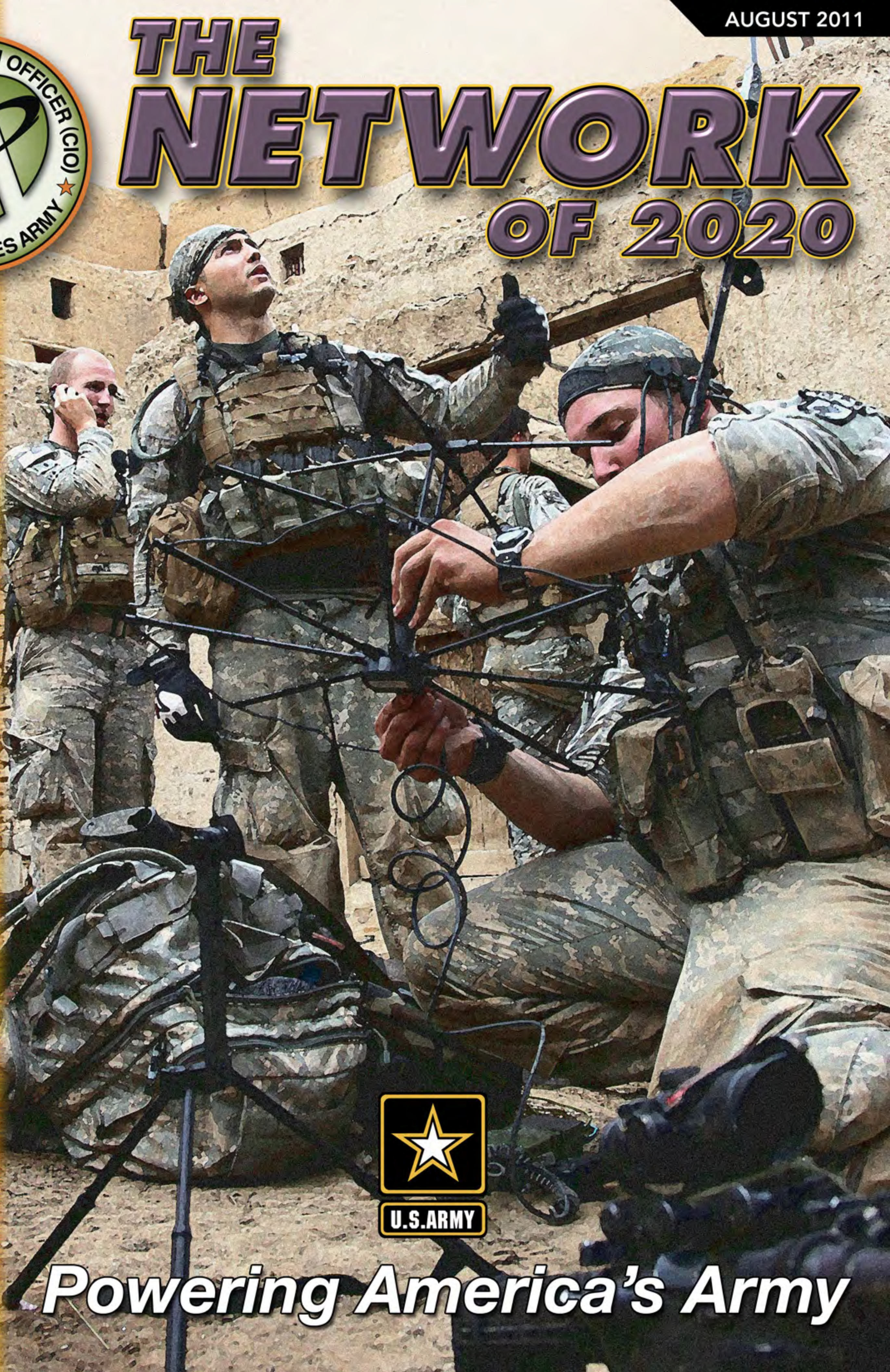
AUGUST 2011

CHIEF INFORMATION OFFICER (CIO)
G-6
UNITED STATES ARMY

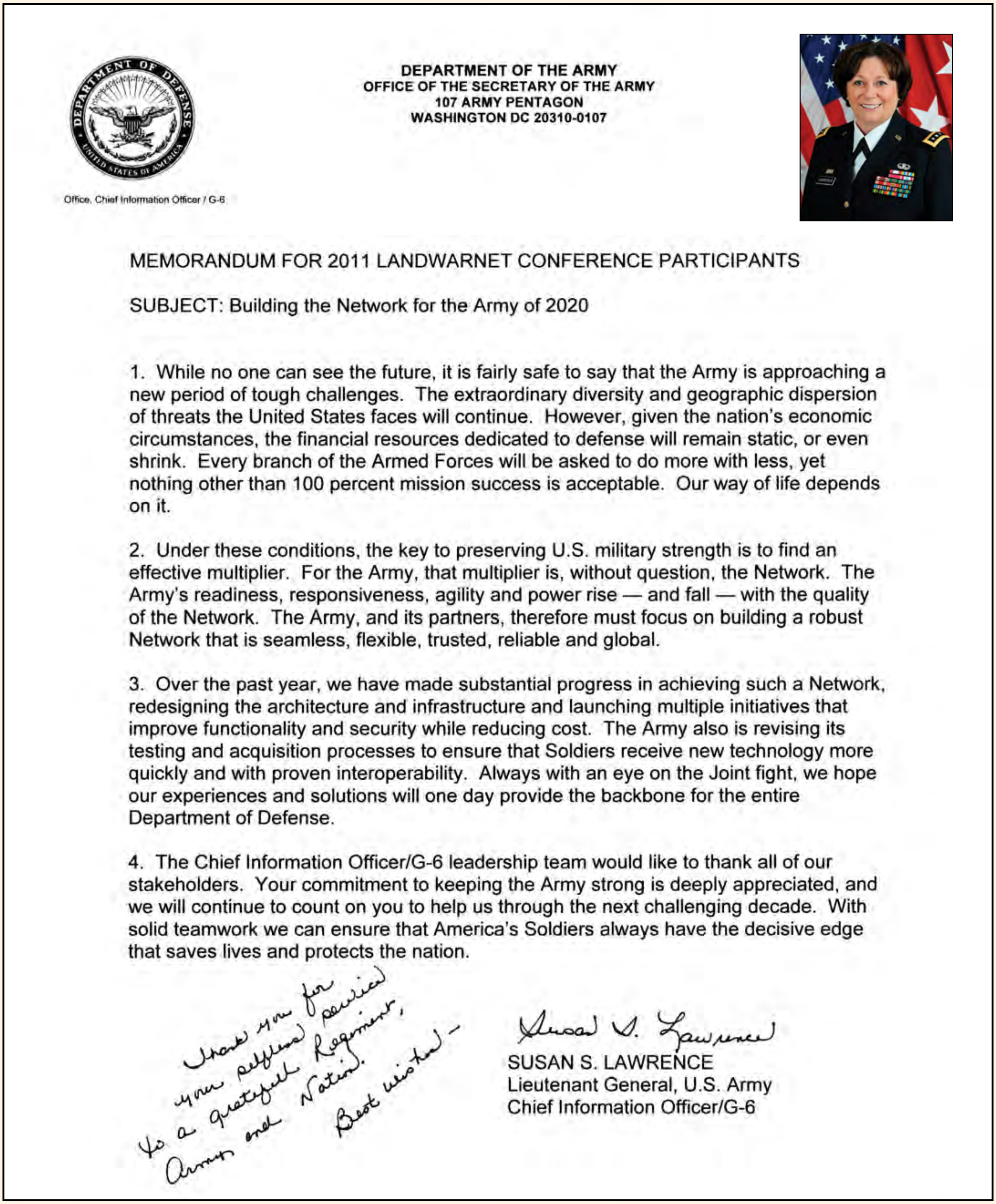
THE NETWORK OF 2020

ARMY CIO/G-6



U.S.ARMY

Powering America's Army



Office, Chief Information Officer / G-6

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

MEMORANDUM FOR 2011 LANDWARNET CONFERENCE PARTICIPANTS

SUBJECT: Building the Network for the Army of 2020

1. While no one can see the future, it is fairly safe to say that the Army is approaching a new period of tough challenges. The extraordinary diversity and geographic dispersion of threats the United States faces will continue. However, given the nation's economic circumstances, the financial resources dedicated to defense will remain static, or even shrink. Every branch of the Armed Forces will be asked to do more with less, yet nothing other than 100 percent mission success is acceptable. Our way of life depends on it.

2. Under these conditions, the key to preserving U.S. military strength is to find an effective multiplier. For the Army, that multiplier is, without question, the Network. The Army's readiness, responsiveness, agility and power rise — and fall — with the quality of the Network. The Army, and its partners, therefore must focus on building a robust Network that is seamless, flexible, trusted, reliable and global.

3. Over the past year, we have made substantial progress in achieving such a Network, redesigning the architecture and infrastructure and launching multiple initiatives that improve functionality and security while reducing cost. The Army also is revising its testing and acquisition processes to ensure that Soldiers receive new technology more quickly and with proven interoperability. Always with an eye on the Joint fight, we hope our experiences and solutions will one day provide the backbone for the entire Department of Defense.

4. The Chief Information Officer/G-6 leadership team would like to thank all of our stakeholders. Your commitment to keeping the Army strong is deeply appreciated, and we will continue to count on you to help us through the next challenging decade. With solid teamwork we can ensure that America's Soldiers always have the decisive edge that saves lives and protects the nation.

Thank you for
your selfless service
to a grateful Regiment,
Army and Nation.
Best wishes –

Susan S. Lawrence

SUSAN S. LAWRENCE
Lieutenant General, U.S. Army
Chief Information Officer/G-6

★★★ The Network ★★★

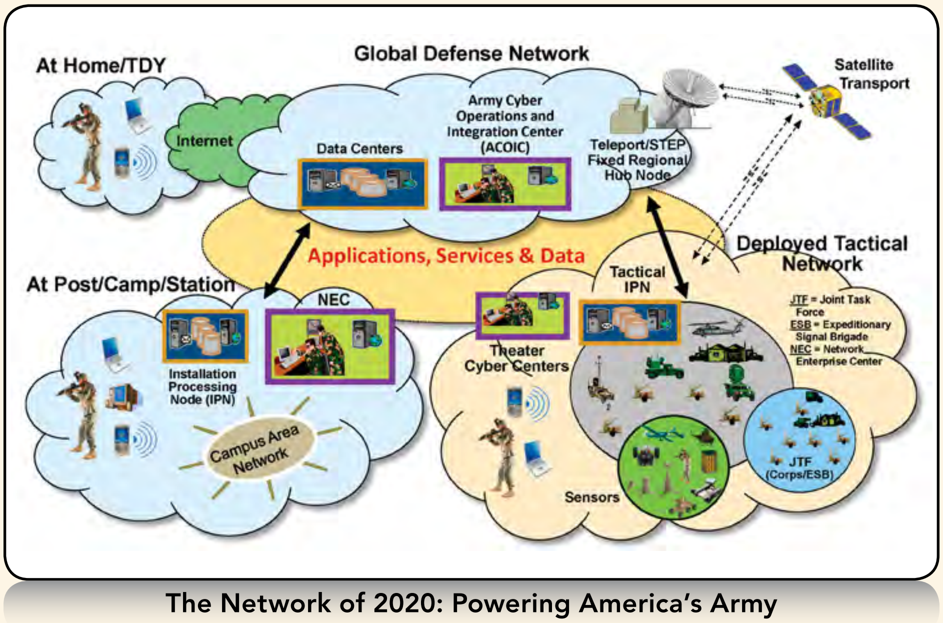
Though no one can see the future, chances are the second decade of the 21st century will look a lot like the first. The threat environment will still feature traditional, though somewhat unpredictable, state actors, as well as the terrorist elements small and large to which we, sadly, have become accustomed. Demand for U.S. troops in overseas operations will remain high, yet the Army will stay based primarily within U.S. borders. The amount of time available to respond to the call for action will continue to shrink, and units will have to hit the ground running. Cutting-edge technology, in particular cyber-related resources, will continue to become cheaper and more widespread, even to those with minimal financial means.

Under these conditions, the Army's relevance to the Joint commander is measured largely by its responsiveness: How fast can the Army deploy, can it bring its full suite of capabilities to bear within the required time frame, and can it maintain the freedom to operate regardless of the challenges it faces?

More and more, the determining factor in whether the Army can meet the Joint commander's, and the nation's, expectations is the Network. Every facet of the expeditionary Army's operations, garrison to the tactical edge, depends upon the Network; its functionality, agility, reliability and security define the chances for success. The challenge, then, is to build a Network that always keeps Soldiers, commanders and civilians connected, informed and empowered. ■

★★★ Network Fundamentals ★★★

As the United States winds down Operations New Dawn and Enduring Freedom, the Army almost certainly will reduce the number of Soldiers on active duty. At the same time, with the entire nation facing a new fiscal reality, the Defense Department budget will shrink. In these circumstances, the Army's mandate will be to produce a force that is smaller yet better trained and more capable. The Network is the key to achieving that Army.


Global Defense Network
At Home/TDY
Internet
Data Centers
Army Cyber Operations and Integration Center (ACOIC)
Teleport/STEP Fixed Regional Hub Node
Satellite Transport
Applications, Services & Data
At Post/Camp/Station
NEC
Installation Processing Node (IPN)
Campus Area Network
Theater Cyber Centers
Tactical IPN
Deployed Tactical Network
JTF = Joint Task Force
ESB = Expeditionary Signal Brigade
NEC = Network Enterprise Center
JTF (Corps/ESB)
Sensors

The Network of 2020: Powering America's Army

For Soldiers, commanders and civilians to be effective, they must always have the right information at the right time, whether in combat, training, conducting homeland defense, providing support to civil authorities, or managing the Army's day-to-day business activities. The Network, therefore, must be global, seamless, always available and always trusted. It must accommodate the functional needs of the entire Army, from infantryman, to logistician, to aviator, to engineer, to resource manager; and facilitate operations in a joint, intergovernmental, interagency and multi-national environment. Furthermore, it must remain on top of the technology curve without breaking the Army's budget.

How will the Army get there from here? Through profound reform of nearly every aspect of Network design, implementation and management. The objective: make construction and operation of the Network easier, more efficient and cheaper, while constantly improving the Network's effectiveness to the end user and its security.

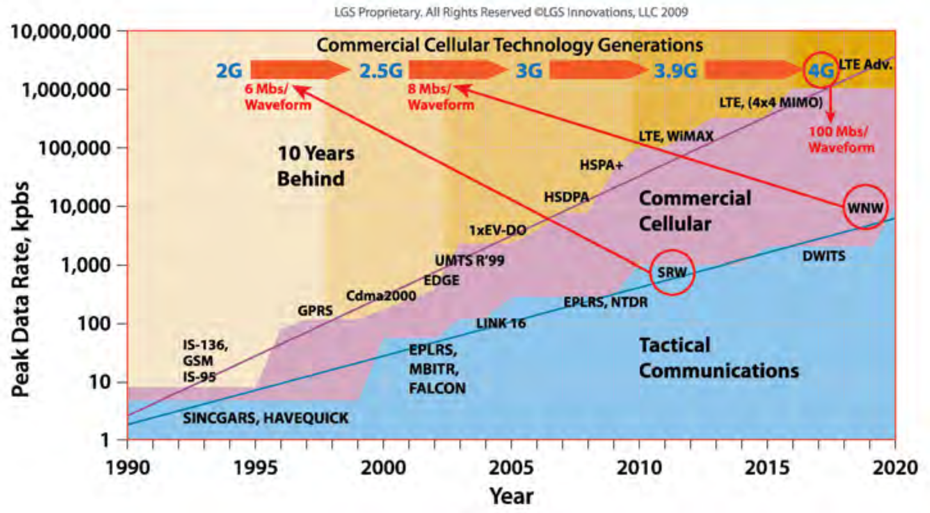
Standardization and centralization are crucial elements of this across-the-board reform. The Army has already applied these principles to the Network's foundation, establishing a uniform basic architecture. The Common Operating Environment (COE) is a centrally approved, commercially based set of computing technologies and standards to which the Network itself and all applications and systems riding the Network must adhere. It defines minimum configurations for the Army's computing environments, from the enterprise server to mobile small handheld devices, and is the key to creating a Network that allows rapid insertion of new technology. Alignment with the COE is now mandatory for new systems and capabilities; the Army is in the process of bringing existing programs of record and non-PORs into compliance, as well.

To solidify the base established by the COE, the Army has also standardized to a single mode of information transmission, regardless of format or delivery means. Whether text, voice, video, signal or other type of data, the Network will move it via a non-proprietary Internet protocol, a method dubbed EoIP (Everything over Internet Protocol).

Getting the right information at the right time requires universal accessibility. The Army, therefore, is also standardizing and centralizing the provisioning of data, applications and services. The most visible efforts include cloud-based enterprise email, collaboration capabilities, directory services and authentication. In addition, the Army's data center consolidation initiative is using a unified cloud-computing operational model to move applications into the DoD cloud as much as possible; then leverage commercial infrastructure; and, as a last resort, utilize Army-owned data centers. (Data centers store, manage and/or disseminate data, information and command, control, communications and computer services to the entire force.) The Army must normalize Network tactics, techniques, procedures and defense, as well. ■

★★★ Eliminating the Gap ★★★

Without question, over the years the Army has frequently failed to keep pace with technology innovation, lagging at least a generation, and often multiple generations, behind what's available in the commercial sector. For the Network to be the effectiveness multiplier the Army needs, the gap must be eliminated – permanently.


LGS Proprietary. All Rights Reserved ©LGS Innovations, LLC 2009

The Need to Change

To start, the Army must better understand its own needs and communicate them to its partners. To that end, the Army is setting an integrated Network capability baseline that will encompass all functional requirements. This baseline, which will be available to industry, will drive the Army's search for specific technologies. As functional needs evolve, so too will the baseline.

The Army's COE-EoIP architecture and refined infrastructure also will go a long way to addressing this disparity. Industry will know in advance the standards to which it must build solutions, which should help to cut the response time, simplify testing and integration, and, possibly, lower costs. Because they are aligned with commercial standards, the COE and EoIP also should enable the Army to commoditize many portions of the Network. Simply put, the Army wants to get out of the information technology research and development business, and rely instead on commercial-off-the-shelf and near-COTS solutions as much as possible. The easier it is to acquire, the faster – and more frequently – the Army can put new capability in Soldiers' hands.

Reforming how the Army delivers Network capability to its operating forces is essential to closing the gap, as well. Traditionally, the Army has developed and fielded Network technologies inefficiently: funding and timelines for Network-related programs were rarely, if ever, aligned; systems were distributed piecemeal; integration with existing technology was largely left up to the user.

The Army is shelving this inadequate, disjointed process in favor of Capability Set Management (CSM). Treating tactical network capability as a cohesive portfolio, Capability Set Management evaluates the current operational environment; designs a suite of systems and equipment to answer the projected requirements of a two-year period; procures any capability not already in inventory; then fields the entire set throughout a combat formation, from the brigade command post to the commander on the move to the dismounted Soldier. Especially significant, Capability Set Management is aligned with Army Force Generation requirements. To further ensure that Soldiers have the most relevant solutions, the Army will buy only enough to fulfill the requirements of any given CSM cycle.

CSM will break with less effective, more time-consuming test and evaluation practices, as well. Rather than execute limited user tests of individual systems, the Brigade Modernization Command will evaluate the entire Capability Set twice prior to fielding, assessing the collective functionality and interoperability of the set, each component's performance and compliance with architectural standards, and whether the set works with existing technology. These robust Network Integration Evaluations (NIE) will replicate the current operational environment and include Soldiers, materiel developers, engineers and trainers.

By relieving the user of the integration burden, new technology is operational when it arrives in his hands – rather than days, weeks or months after the unit has figured out how to incorporate it with existing systems. Already, the NIE conducted in July prevented the fielding of a system that, if sent down range as is, would not have been functional. And, because the right mix of personnel were present at the evaluation, the adjustments necessary to make it operable were determined.

The NIE is part of a larger change in Army acquisition practices geared toward enabling rapid technology insertion. Known as the Agile Process, this new approach focuses on meeting identified and prioritized capability gaps by integrating emerging technological solutions through iterative, pre-defined, predictable windows of testing and insertion, all in alignment with ARFORGEN. In examining potential technologies, the Agile Process will take into account maturity and cost. It will use Network Integration Rehearsals to assess systems and concepts, and full Network Integration Evaluations to generate user recommendations regarding system/concept continuance and any DOTMLPF modifications necessary for integration with existing technology, tactics, techniques and procedures. ■

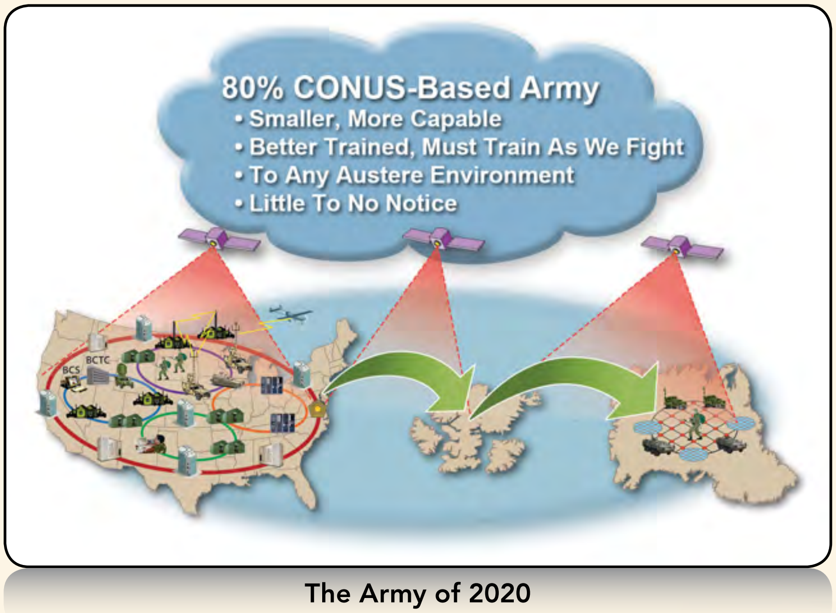
> "We must fundamentally change how we acquire IT.
> We can't just close the technology gap — we must eliminate it."
> *– LTG Susan S. Lawrence, Army CIO/G-6*

Train As We Fight

For a smaller Army to be as, or more, effective on the battlefield, Soldiers must be completely prepared to engage the moment they enter the area of operations. That means having full situational awareness and understanding before arriving in theater. The Network is the medium for sharing this crucial knowledge.

The Army has already proven the concept – and the enormous benefit – of extending the battlespace to next-deployers while they are still at home station. By supplying access to the coalition Afghanistan Mission Network (through the United States' portion, known as the Combined Enterprise Regional Information Exchange System – International Security Forces Afghanistan or CENTRIXS-ISAF), units readying to deploy participate in the daily intelligence and operations updates. As a senior commander recently put it: this is a "game changer". Without question, this type of capability must become a staple of all future Army, and Department of Defense, engagements.

Soldiers who truly can fight upon arrival must already be familiar with all of the systems and technologies they will use in the battlespace. However, today the only time a warfighter can train on key mission command applications is when he or she is in the field on the tactical network. Classroom 2020 will erase this limitation, creating a computing environment that places critical applications, such as Command Post of the Future, the Advanced Field Artillery Tactical Data System and Force XXI Battle Command, Brigade and Below, in the classroom, motor pool or orderly room. Soldiers will be able to train as they fight while still in garrison, giving them a leg up when they finally do deploy and in the meantime allowing them to go home at night to their families. ■



The Army of 2020

★★★ One Playbook ★★★

Over time, the number of documents guiding and regulating IT has multiplied to the point of confusion, and the number of people with Network-related decision-making authority has swelled. Some of this growth can be attributed to 10 years of persistent war. Regardless of the cause, it is in no way beneficial. Recent examination has revealed a detrimentally "dirty" Network environment.

For the Network to be reliable and trusted, the Army must tighten IT governance and policies. The first step is to trim significantly (by more than 50 percent) the number of personnel Army-wide with the authority to make decisions that can affect the integrity, functionality and security of the Network. While this select group will be able to call some of the plays, the Chief Information Officer/G-6 will remain the single IT authority for Title 40 (the Clinger-Cohen Act) and Title 44.

The second is to eliminate the plethora of publications, from memoranda to formal policies to interim updates, that govern information technology. The Army cannot reasonably expect its commanders to operate and maintain the Network properly without a definitive playbook. The CIO/G-6 therefore intends to consolidate to just two authoritative sources: Army Regulation 25-1 and Army Regulation 25-2. To ensure that these documents reflect the current state of technology and Army TTPs, they will be updated annually. In addition, CIO/G-6 will strengthen compliance enforcement. ■

★★★ Help From Our Partners ★★★

The Army cannot produce the Network commanders and Soldiers need without help from our executive branch, legislative branch and industry partners. To tap commercial technology and keep Network capabilities fresh and relevant, the Army will require greater funding flexibility. Today's appropriations dollars often do not arrive at the start of the fiscal year but always expire at the end of it, impacting the Army's ability to stay on top of the technology market and buy exactly what is needed in the order it is needed. Three-year funding, and modified federal acquisition rules, would enable the Army to be more responsive to Soldiers' needs and to provide them more capable solutions.

To achieve the Network that is always on, always accessible, always able to carry and transmit the information requested, yet always secure, the Army will need the best minds in academia and industry. The Army recognizes that specific technological challenges lie ahead, such as adequate bandwidth and competition for spectrum. Ideas from anyone in the IT community regarding how to address these issues are warmly welcomed. More generally, the Army wants our non-governmental partners to tell us what you see on the horizon. What is the transformational thing that the Army has not yet thought about? What is the next smart device that will change the way we operate; what is the next tool that will enhance Network security; where will society be technologically five to seven years from now? Only if the Army is aware of what is possible, what may be on the technology roadmap, can we make the right design, resourcing and acquisition decisions – and never again fall into the technology gap. ■

★★★ To the Army of 2020 ★★★

As the blueprint for the Network evolves, the Army and its partners must be careful to take into account the joint and coalition nature of the operational environment. Only if we incorporate a broader net-centric perspective will DoD attain real interoperability, avoid duplicative efforts, reduce security risk and stay within budget. To that end, the Army is prepared to focus on developing a joint integrated architecture and end-to-end systems engineering for all Defense Department networks.

For the unified Network to be effective, the Army also will have to change its culture. Commanders and Soldiers must have confidence that the Network will always be on and always provide them what they need – that the whole Army can safely rely upon one central service provider. Getting the physical engineering and the mix of capabilities right will go a long way to establishing that trust. Senior leadership must play a part, too.

The president, the Congress and the American people are counting on the Army to remain the best land force in the world. With the Network as the No. 1 modernization effort, the Army will have the power, versatility and agility necessary to fulfill this mandate. The Chief Information Officer/G-6 is firmly committed to making sure that the Network keeps the Army, and the entire Joint Force, indomitable. ■

U.S.ARMY

AMERICA'S ARMY:
THE STRENGTH OF THE NATION™

Army Chief Information Officer/G-6
107 Army, Pentagon
Washington, DC 20310
CIOG6.Army.mil